ABSTRAK

Keamanan merupakan aspek terpenting dalam membangun *server* layanan jaringan. *Port* layanan jaringan yang terbuka dapat mengakibatkan *server* dapat diakses oleh siapapun, sehingga *user* yang tidak berkepentingan dapat mengakses *server* layanan jaringan. *Server* juga rentan untuk diretas dengan mudah. Oleh karena itu pada saat membangun layanan jaringan pada *server* harus disertai *firewall* dan keamanan yang memadai. Bertujuan untuk mengurangi terjadinya peretasan atau hacking pada layanan jaringan yang sudah dibangun di *server*. Layanan jaringan tersebut akan dibangun di sistem operasi Linux Ubuntu 14.04. Pengamanan *port* layanan jaringan, menggunakan metode *port knocking* untuk melakukan autentikasi sebelum mengakses *server* dan dikombinasikan dengan fitur *firewall* IP *filter* dan *packet timeout* di router Mikrotik. Dimana metode tersebut akan memilih IP yang diijinkan untuk mengakses *server*. Metode tersebut akan diimplementasikan di *firewall* router Mikrotik, supaya dalam pembangunan layanan jaringan pada *server* lebih aman dan mengurangi terjadinya peretasan. Dalam penelitian ini penulis menggunakan metode pengerjaan *waterfall* supaya memudahkan dalam proses pengerjaan. Hasil dari penelitian ini adalah terbentuknya sistem autentikasi dan keamanan pada *server* layanan jaringan menggunakan metode *port knocking* dan *firewall* di router Mikrotik. Dengan penelitian ini diharapkan dapat menjadi solusi keamanan *server* layanan jaringan yang rentan untuk diretas.

Kata Kunci : Mikrotik, *Port knocking*, Keamanan Jaringan, IP *filter*, *Packet timeout*.